CLAIMS

What is claimed is:

1. A traffic management system for use in conjunction with packet data, said system operative for passing data packets there through, said system comprising:

means for extracting certain parameters of data from each packet of data which is flowing into said system; and

means for comparing said extracted data against at least one database to determine if the data packet associated with said extracted data is valid.

2. The traffic management system of claim 1 wherein said extracted data includes the software and hardware address of the originator of said packet.

3. The traffic management system of claim 2 wherein a network database is queried for each packet based upon the extracted address information of said packet.

4. The traffic management system of claim 2 further including:

a local database wherein extracted ones of said hardware and software addresses are stored.

5. The traffic management system of claim 4 wherein said comparing means compares the extracted hardware and software address pairs from each packet against said stored address into data in said local database.

6. The traffic management system of claim 1 wherein said extracting means extracts sequencing data and/or time stamp data for said packets.

7. The traffic management system of claim 5 further including:

a local database wherein extracted ones of said sequencing and/or time stamp data is stored.

8. The traffic management system of claim 7 wherein said comparing means compares the extracted sequences and/or time stamp data from each packet against said stored sequence and/or time stamped data in said local database.

9. A data network monitoring system comprising:

at least one data sniffer;

a temporary storage device;

a processor for determining spoofing with respect to data passing through said system; and

said processor further operative for diverting to said temporary storage device selected data entering said system, said selected data controlled in part by information obtained from said data sniffer and from a determination of spoofing.

10. The data network monitoring system of claim 9 wherein said system further comprises a store of data having undesirable characteristics, and wherein said processor operates to compare said store of undesirable data with data obtained from said data sniffer to assist in said spoofing determinations.

11. The data network monitoring system of claim 9 further comprising a display for displaying in real time certain parameters pertaining to spoofing.

12. The method of controlling a traffic management system, said method comprising the steps of:

reviewing certain parameters of data packets flowing into said system, said parameters pertaining to possible spoofing;

remembering for a period of time said reviewed certain parameters in conjunction with each received data packet; and

upon attainment of packet flow volume into said system reaching a certain level, temporarily storing certain subsequently received packets in accordance with selective remembered parameter of previously received packets.

13. The method of claim 12 wherein said certain level is user controlled.

14. The method of claim 12 wherein said certain level includes a plurality of levels, wherein the attainment of each successive level results in a more stringent application of said remembered certain parameters.

15. The method of claim 12 wherein said remembered parameters include one or more of: a sender's software address; a sender's hardware address; a prior trouble causing address; a notice of a potential trouble address; amount of data transmitted from a particular address in a period of time; number of packets arriving from a particular address in a period of time; an address' domain name; date of initial encounter with an address; date of latest encounter with an address, a sequence number of a transaction; a time stamp of a transaction.

16. The method of claim 15 wherein said certain level includes a plurality of levels arranged in a sequence, and wherein as the sequence of levels gets closer to an absolute maximum data flow rate more and more of said remembered parameters are included as a basis for said determination to temporarily store a particular packet.

17. The method of claim 16 further including the step of:

arbitrarily selecting packets for temporary storing when said data flow rate reaches its maximum capacity.

18. The method of claim 12 further including the step of:

retrieving said temporarily stored data packets when traffic flow into said system falls below said certain level.

19. The method of claim 26 further including the step of:

putting at least some of said retrieved data packets through said system.

20. The method of claim 12 further comprising the step of:

dynamically displaying information pertaining to temporarily stored ones of said data packets.

21. The method of claim 20 wherein said displaying step includes:

transmitting said display information to a remote location.

22. A method for preventing data from flowing beyond a particular point faster than the handling capability associated with that point; said system comprising the steps of:

remembering certain parameters of data passing said particular point, said certain parameters selected from the list of: software address of a sender; hardware address of a sender; time stamp of a transaction; sequence of a transaction; data pertaining to spoofing; and

preventing selected data from passing said particular point when the data handling capability associated with that point reaches a preset limit, said preventing step relying on said remembered parameters pertaining to data previously passing said particular point.

23. A data flow control system for preventing an enterprise data processing system from being overloaded with spoofed data requests directed to said enterprise system from sources external to said enterprise system, said data flow system comprising:

a gateway for accepting data directed to said enterprise system from any said external source;

a data monitoring circuit for observing selected portions of certain data directed to said gateway, and

a delay path operable when the amount of data currently being handled by said enterprise system reaches a certain threshold for temporarily removing selected data which is directed to said enterprise system away from enterprise system, said selected data having an uncertain probability of spoofing.

24. The system of claim 23 wherein the exact ones of said data which are temporarily removed are selected under control of information provided by said data monitoring circuit.

25. The system of claim 23 wherein said certain threshold has gradations and wherein the amount and types of data that are temporarily removed operate in proportion to said gradations.